О НЕПРИВОДИМОСТИ ПОЛИНОМОВ СПЕЦИАЛЬНОГО ВИДА НАД КОНЕЧНЫМИ ПОЛЯМИ

Валуева Т.А., БГУ, Минск

Рассмотрим f(x) — неприводимый полином степени n над полем F_p, $\mathrm{ordf}(x)=\frac{p^n-1}{s}$, где s — некоторый делитель числа p^n-1. Будем исследовать неприводимость полинома $f(x^T)$, T > 1. В работе [

1] доказано, что если все простые делители числа T делят порядок f(x) и выполняются некоторые дополнительные условия, то полином $f(x^T)$ является неприводимым. В статье [4] получены необходимые и достаточные условия неприводимости полиномов вида $x^{p^n}+ax+b$ над полем F_p. В данной статье получен критерий неприводимости полиномов вида $f(x^T)$ над полем F_p.

Отметим, что в поле $GF(p^n)$ полином f(x) имеет n корней: $\alpha,\alpha^p,...,\alpha^{p^{n-1}}$. Все корни полинома $f(x^T)$ являются корнями полиномов $x^T-\alpha^{p^i}$, $i=\overline{0,n-1}$. Полином $f(x^T)$ неприводим над полем F_p тогда и только тогда, когда полиномы $x^T-\alpha^{p^i}$, $i=\overline{0,n-1}$ неприводимы над полем $GF(p^n)$.

Лемма 1. *Если полином $x^T-\alpha^{p^i}$ для некоторого $i=\overline{0,n-1}$ имеет корень в поле $GF(p^n)$, то все полиномы $x^T-\alpha^{p^i}$, $i=\overline{0,n-1}$ имеют корень в поле $GF(p^n)$ порядка $\frac{p^n-1}{s}$.*

Лемма 2. *Для всех $i=\overline{0,n-1}$ полиномы $x^T-\alpha^{p^i}$ имеют корень в поле $GF(p^n)$ тогда и только тогда, когда НОД($\frac{T}{d},\frac{p^n-1}{s}$)=1, где d=НОД(T,s).*

Доказательства лемм **1**, **2** аналогичны доказательствам лемм 1,2 в [2].

Лемма 3. *Полиномы $x^T-\alpha^{p^i}$, $i=\overline{0,n-1}$ неприводимы над полем $GF(p^n)$ тогда и только тогда, когда все простые делители числа T делят число $\frac{p^n-1}{s}$, не делят s, и $p^n\equiv 1(mod4)$, если T кратно 4.*

Доказательство. Докажем достаточность условий леммы. В силу леммы **1** достаточно рассмотреть полином $x^T-\alpha$. Из теоремы 16[3] следует, что данный полином неприводим над полем $GF(p^n)$ если для всех простых p_i, делящих T, $\alpha\notin GF(p^n)^{p_i}$ и $\alpha\notin -4GF(p^n)^4$ в случае, когда T кратно 4. $GF(p^n)^{p_i}$ — множество, состоящее из элементов поля $GF(p^n)$ в p_i-й степени. Докажем, что $\alpha\in GF(p^n)^{p_i}$ тогда и только тогда, когда. p_i не делит $\frac{p^n-1}{s}$ или p_i делит s.

Пусть γ — образующий мультипликативной группы поля $GF(p^n)$, тогда $\alpha=\gamma^{s\cdot m}$, причем НОД(m,p^n-1)=1. Предположим, что $\alpha\in GF(p^n)^{p_i}$. Следовательно, существует такое k, что $(\gamma^k)^{p_i}=\gamma^{s\cdot m}$, что равносильно тому, что относительно k разрешимо следующее сравнение:

$$p_i\cdot k\equiv s\cdot m(\mathrm{mod}\,p^n-1). \qquad (1)$$

Согласно лемме **2** сравнение ((1)) разрешимо тогда и только тогда, когда НОД($\frac{p_i}{d}, \frac{p^n-1}{s}$)=1, где d=НОД($p_i$,s). Учитывая, что p_i — простое, рассмотрим следующие случаи.

1) p_i не делит s, тогда сравнение ((1)) разрешимо тогда и только тогда, когда p_i не делит $\frac{p^n-1}{s}$.

2) p_i делит s, тогда НОД($\frac{p_i}{d}, \frac{p^n-1}{s}$)= 1, т.е. сравнение ((1)) всегда разрешимо.

Рассмотрим случай, когда T кратно 4. В случае, когда p=2, полином $f(x^T)=f(x^{4t})=f^4(x^t)$— приводим над полем F_2. Поэтому будем рассматривать p>2. Условие $\alpha \notin -4GF(p^n)^4$ равносильно условию $\alpha \notin (p-4)GF(p^n)^4$. Пусть, как и ранее, γ-образующий мультипликативной группы поля GF(p^n), тогда $\alpha=\gamma^{s\cdot m}$ и $\gamma^{p^n-1}=1$. Так как НОД(p-4, p) =1, то $(p-4)^d$ =1, где d — показатель, которому принадлежит (p-4) по модулю p. Тогда $\gamma^{\frac{p^n-1}{d}}=p-4$. Предположим, что $\alpha \in (p-4)GF(p^n)^4$. Следовательно, существует такое k, что $\gamma^{\frac{p^n-1}{d}}\gamma^{4k}=\gamma^{s\cdot m}$, что равносильно тому, что относительно k разрешимо следующее сравнение:

$$s\cdot m \equiv 4k+\frac{p^n-1}{d}(\mathrm{mod}\, p^n-1) \qquad (2)$$

Рассуждая аналогично, как при решении сравнения ((1)); получим, что сравнение ((2)) разрешимо тогда и только тогда, когда $p^n \equiv 3(\mathrm{mod}\, 4)$.

Таким образом, если все простые делители числа T делят $\frac{p^n-1}{s}$, не делят s, и $p^n \equiv 1(\mathrm{mod}\, 4)$, в случае, когда T кратно 4, то полином $x^T-\alpha$ является неприводимым полиномом над полем GF(p^n), а полином $f(x^T)$ — неприводим над полем F_p.

Покажем необходимость условий леммы.

Докажем, что если существует простой делитель p_i числа T, который является взаимно простым с $\frac{p^n-1}{s}$ либо делит s, то полином $f(x^T)$ приводим над полем F_p.

Вычислим d = НОД(T,s). Пусть $T=p_1^{\gamma_1}\cdot p_2^{\gamma_2}\cdot \ldots \cdot p_m^{\gamma_m}$ — каноническое разложение числа T. Положим $r_1=p_{i_1}^{\gamma_{i_1}}\cdot p_{i_2}^{\gamma_{i_2}}\cdot \ldots \cdot p_{i_k}^{\gamma_{i_k}}$, где $p_{i_j}, j=\overline{1,k}$ делят s. Тогда d = НОД(T,s) = НОД(r_1,s). Положим $r_2=p_{j_1}^{\gamma_{j_1}}\cdot p_{j_2}^{\gamma_{j_2}}\cdot \ldots \cdot p_{j_n}^{\gamma_{j_n}}$, где $p_{j_i}, i=\overline{1,n}$ делят числа $\frac{p^n-1}{s}$ и $\frac{T}{r_1}$. Пусть $r=\frac{r_1\cdot r_2}{d}$, $t=\frac{T}{r}=\frac{T}{r_1\cdot r_2}\cdot d$. Отметим, что НОД(T,s) = НОД(t,s), в число t входят d и все простые p_i в соответствующих степенях, которые не делят $\frac{p^n-1}{s}$.

Полином $x^T-\gamma^{s\cdot m}$ представим следующим образом: $x^T-\gamma^{s\cdot m}=x^{r\cdot t}-\gamma^{s\cdot m}=y^t-\gamma^{s\cdot m}$.

Т.к. НОД(t,s) = d и НОД($\frac{t}{d}, \frac{p^n-1}{s}$)= 1, из лемм **1**, **2** получим, что полином $y^t - \gamma^{s\cdot m}$ имеет корень в поле GF(p^n) порядка $\frac{p^n-1}{s}$, т.е. $y^t - \gamma^{s\cdot m} = (y-\iota)\cdot g(y) = (x^r-\iota)\cdot g(x^r)$. Тогда $f(x^T) = \prod_{i=0}^{n-1}(x^T - \alpha^{p^i}) = \prod_{i=0}^{n-1}(x^r - \iota^{p^i})\cdot\ g_i(x^r) = h(x^r)\cdot g(x^r)$, где h(x) — неприводимый полином степени n.

Рассмотрим случай, когда $\alpha \in -4GF(p^n)^4$ и T кратно 4. Пусть $\alpha = -4\beta^4$, T=4t, тогда $x^T - \alpha = x^{4t} - \alpha = [y = x^t] = y^4 + 4\beta^4 = (y^2 + 2\beta y + 2\beta^2)\cdot (y^2 + +(p-2)\cdot\beta + 2\beta^2)$— приводим над GF($p^n$), и следовательно, полином f(x^T) — приводим над F_p.

Из лемм **1**,**2**,**3** следует справедливость следующей теоремы:

Теорема 1. *Пусть f(x) — неприводимый полином над полем F_p степени n, $ordf(x) = \frac{p^n-1}{s}$. Полином f($x^T$) является неприводимым над полем F_p тогда и только тогда, когда все простые делители числа T делят число $\frac{p^n-1}{s}$, не делят число s, и $p^n \equiv 1(mod4)$, если T кратно 4.*

Литература

1. Лидл Р., Нидеррайтер Г. Конечные поля, т.1, М.: Мир, 1988.
2. Валуева Т.А. О приводимости одного класса полиномов, Информационные системы и технологии — IST'2002, 2ч., стр.15-16.
3. Ленг С. Алгебра, М.: Мир, 1967.
4. Chen Song-Liang Some trinomials over finite prime fields, J. Jinzhou Norm. Coll. Natur. Sci. Ed., 2002, №1, p. 65-66.

ЧИСЛЕННОЕ РЕШЕНИЕ ИНТЕГРАЛЬНЫХ УРАВНЕНИЙ В МУЛЬТИВЕЙВЛЕТНОМ И ТРИГОНОМЕТРИЧЕСКОМ БАЗИСАХ

Герасимчик И.В., Дейцева А.Г., ГрГУ, Гродно

В данной работе рассмотрено интегральное уравнение Фредгольма второго рода

$$y(x) - \int_0^1 K(x,s)y(s)ds = f(x), \qquad (1)$$

где $K(x,s) \in L_2[0;1]^2$, $f(x) \in L_2[0;1]$, $x \in [0;1]$ –известные функции, $y(x)$, $x \in [0;1]$ – неизвестная функция.

Пусть $\{b_1(x), b_2(x), \ldots\}$ – ортонормированный базис в $L_2[0;1]$. Тогда для функций из уравнения (1) справедливы следующие разложения

$$K(x,s) = \sum_{i=1}^{\infty}\sum_{j=1}^{\infty} K_{ij} b_i(x) b_j(s), \qquad (2)$$